The Fuzzing Project
https://fuzzing-project.org/

Hanno Böck

strings, file, less

- Did you expect to be owned by file, strings or less?
- You should!

What is Fuzzing?

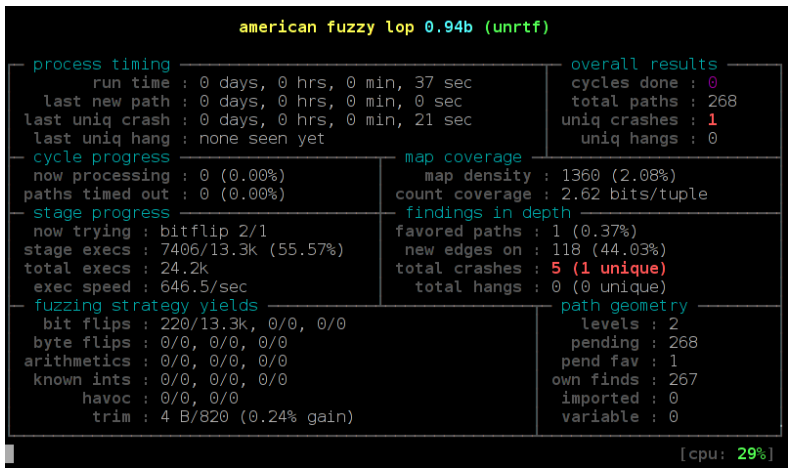
- Take a valid input, add random errors, feed software with it
- If software crashes (or shows other undesired behaviour) you found a bug
- Crashes very often memory access issues, potential security threats

State of our software base

- Pick a random free software tool that parses files, fuzz it
- Chances are high you'll find bugs within seconds

Tools

- Address Sanitizer: compiler flag that enables better bounds checking - highly effective in finding memory access issues
- american fuzzy lop: intelligent fuzzer with compile time instrumentation - already found dozends of issues, often in security sensitive software (GnuPG, libjpeg, bash, ...)



The Fuzzing Project

- Some loose coordination and documentation of fuzzing efforts, list of free software projects and their fuzzing robustness
- Tutorial for beginners
- Small sample files archive
- Goal: Wipe out bugs that can be trivially found by fuzzing

What you can do

- If you are a software developer: Make fuzzing part of your development process
- If you care about free software security: Help us fuzz everything

`https://fuzzing-project.org/`